Guide de sécurité SIL

PolyTrans® P32000P0/1*

ThermoTrans® P32100P0/1*

SensoTrans® P32200P0/1*

SensoTrans® P32300P0/1*

www.knick.de

80115

Knick

Table des matières

1 Champ d'application et normes 4
1.1 Abréviations 6
2 Descriptif de l'appareil et champ d'application 8
2.1 Fonction de sécurité 8
2.2 Définition de l'état sûr 8
3 Informations relatives à la programmation 9
3.1 Mode de fonctionnement à faible taux de demande 9
3.2 Mode de fonctionnement à taux de demande élevé 9
3.3 Types d'erreur 9
3.4 Intervalle d'essai de diagnostic 10
4 Montage et installation 11
5 Contrôles périodiques 13
5.1 Vérification du fonctionnement 13
6 Caractéristiques de sécurité 15
6.1 Suppositions 15
6.2 Caractéristiques spécifiques de sécurité 16
6.3 Exemple de calcul 17
7 Certificat 19

1 Champ d'application et normes

Ce guide de sécurité concerne les convertisseurs des séries PolyTrans® P32000P0/1∗, ThermoTrans® P32100P0/1∗, SensoTrans® P32200P0/1∗ et SensoTrans® P32300P0/1∗.

Versions matérielles et logicielles valides :

- Numéros de série à partir de 1657362
- Logiciel de l'appareil à partir de la rév. 1.28 / 2.0

Les convertisseurs orientés sécurité de la série P32xxxP0/1∗ de Knick Elektronische Messgeräte GmbH & Co. KG sont certifiés SIL 2 (SIL 3 en cas de câblage redondant) par le TÜV, conformément à la norme EN 61508 :

TÜV Rheinland Industrie Service GmbH
Automation, Software und Informationstechnologie (ASI)
Am Grauen Stein
D - 51105 Cologne

Functional Safety
Type Approved
TÜVRheinland® FS

N° du certificat et du rapport d'essai : 968/EZ 272.00/07

Les convertisseurs sont développés et contrôlés conformément aux normes suivantes :

- **EN 61508 : 2001**
  Sécurité fonctionnelle des systèmes électriques/électroniques/ programmables de sécurité
- **EN 61511 : 2004**
  Sécurité fonctionnelle – Systèmes de sécurité pour l'industrie des processus
- **EN 61010-1 : 2001**
  Contraintes de sécurité pour les appareils électriques de mesure, de commande, de régulation et de laboratoire
- **EN 61326-1 : 2006**
  Appareils électriques de mesure, de commande, de régulation et de laboratoire – Exigences CEM
- **EN 61326-2-3 : 2006**
  Appareils électriques de mesure, de commande, de régulation et de laboratoire – Exigences CEM – Partie 2-3 : Exigences particulières – Disposition de contrôle, conditions de fonctionnement et caractéristiques de puissance des convertisseurs avec traitement des signaux intégré ou amovible
- **IEC 61326-3-2 : 2006**
  Appareils électriques de mesure, de commande, de régulation et de laboratoire – Exigences CEM – Partie 3-2 : Exigences d'immunité pour les appareils qui exécutent des fonctions de sécurité ou qui sont utilisés pour des fonctions de sécurité (sécurité fonctionnelle) – Applications industrielles dans des environnements électromagnétiques
- **EN 50178 : 1997**
  Equipement électronique des installations à courant fort

1.1 Abréviations

Abréviation	Anglais	Français
SIL	Safety Integrity Level	La norme internationale IEC 61508 définit quatre niveaux d'intégrité de sécurité (Safety Integrity Level) discrets (de SIL 1 à SIL 4). Chaque niveau correspond à une plage de probabilité de défaillance d'une fonction de sécurité. Plus le niveau d'intégrité de sécurité des systèmes de sécurité est élevé, plus il est probable qu'ils exécutent efficacement les fonctions de sécurité demandées.
PFD	Probability of Failure on Demand	Probabilité de défaillance dangereuse d'une fonction de sécurité en cas de demande
PFD_G	Average Probability of Failure on Demand	Probabilité moyenne d'une défaillance dangereuse en cas de demande d'un groupe de canaux avec comparateur de sortie ou élément de décision à la majorité
PFH	Probability of a dangerous Failure per Hour	Probabilité de défaillance de la fonction de sécurité par heure
PFH_G	Average Probability of a dangerous Failure per Hour	Probabilité de défaillance par heure pour un groupe de canaux avec comparateur de sortie ou élément de décision à la majorité
SFF	Safe Failure Fraction	Part de défaillances non dangereuses : Part de défaillances n'entraînant pas le basculement du système de sécurité dans un état de fonctionnement dangereux ou non autorisé
λ_S	Rate of safe failures	Taux de défaillances non dangereuses par heure
λ_D	Rate of dangerous failures	Taux de défaillances dangereuses par heure
λ_{DU}	Rate of dangerous undetected failures	Taux de défaillances dangereuses non détectées par heure
λ_{DD}	Rate of dangerous detected failures	Taux de défaillances dangereuses détectées par heure
DC	Diagnostic Coverage of dangerous failures	Degré de couverture du diagnostic : $DC = \lambda_{DD} / (\lambda_{DU} + \lambda_{DD})$
HFT	Hardware Fault Tolerance	Tolérance d'erreurs du matériel : Capacité d'une unité fonctionnelle à continuer à exécuter une fonction demandée en cas d'erreur ou d'écart

Abrévia-tion	Anglais	Français
MTBF	Mean Time Between Failures	Temps moyen entre deux défaillances
MTTR	Mean Time To Repair	Temps moyen entre l'apparition d'une erreur dans un appareil ou un système et la résolution
FIT	Failure In Time	1 x 10^{-9} erreurs par heure
TI	Test Interval between life testing of the safety function	Intervalle de contrôle entre les essais de fonctionnement de la fonction de protection
XooYD	X out of Y Voting (e.g. 1oo2)	Classification et description du système de sécurité sur le plan de la redondance et du mode de sélection utilisé. "Y" indique la fréquence à laquelle la fonction de sécurité est exécutée (redondance). "X" indique le nombre de canaux qui doivent fonctionner correctement. Exemple de mesure de la température : architecture 1oo2. Le système de sécurité décide qu'une limite de température prédéfinie est dépassée lorsque l'un des deux capteurs de température atteint cette limite. Dans une architecture 1oo1, un seul capteur de température est installé. "D" indique que le système inclut une fonction de diagnostic.
t_{CE}	Channel Equivalent mean down time	Temps moyen d'indisponibilité d'équivalence (en heures), temps d'indisponibilité commun pour tous les composants dans un canal du sous-système
t_{GE}	Voted Group Equivalent mean down time	Temps moyen d'indisponibilité d'équivalence (en heures) pour un groupe avec comparateur de sortie ou élément de décision à la majorité, temps moyen d'indisponibilité pour tous les canaux dans un groupe avec comparateur de sortie ou élément de décision à la majorité

2 Descriptif de l'appareil et champ d'application

2.1 Fonction de sécurité

Les convertisseurs transmettent les valeurs d'entrée dans un signal de sortie analogique normalisé de 0/4 à 20 mA ou de 0 à 5/10 V avec une isolation galvanique. La fonction de transmission peut être ajustée aux capteurs raccordés à l'entrée. Le signal de sortie analogique est retransmis à une unité logique (par ex. un API).

Dans une architecture monocanal (1oo1), les appareils peuvent être utilisés jusqu'à SIL 2. Dans une architecture multicanal redondante, ils peuvent être utilisés jusqu'à SIL 3. Les signaux de sortie des convertisseurs doivent être surveillés par un équipement approprié en amont (par ex. fonction de surveillance dans un API) et de manière orientée vers la sécurité comme un 'système 1 sur 2' au sens de la norme DIN EN 61508 (cf. DIN EN 61508-6, B.2.2.2).

2.2 Définition de l'état sûr

Type de signal de sortie	Etat sûr
0 – 20 mA	≤ 3,6 mA ; ≥ 21 mA
4 – 20 mA	≤ 3,6 mA ; ≥ 21 mA
0 – 10 V	≤ 0,1 V ; ≥ 10,5 V
0 – 5 V	≤ 0,1 V ; ≥ 5,25 V

3 Informations relatives à la programmation

3.1 Mode de fonctionnement à faible taux de demande

Les convertisseurs sont utilisés en mode de fonctionnement à faible taux de demande (low demand mode) lorsque le taux de demande auprès des convertisseurs ne dépasse pas une fois par an et ne dépasse pas le double de la fréquence du contre-essai (DIN EN 61508-4, 3.5.12).

Le mode de fonctionnement à faible taux de demande peut aussi être utilisé lorsque le rapport entre le taux d'essais de diagnostic interne du convertisseur et le taux de demande ne dépasse pas la valeur 100 (DIN EN 61508-2, 7.4.3.2.5).

La caractéristique correspondante est la valeur PFD. La valeur dépend de l'intervalle de contrôle TI entre les essais de fonctionnement de la fonction de protection.

3.2 Mode de fonctionnement à taux de demande élevé

Si le "mode de fonctionnement à faible taux de demande" n'est pas approprié, utiliser le convertisseur comme un sous-système de sécurité en mode de fonctionnement à taux de demande élevé ou continu (high demand or continuous mode) (DIN EN 61508-4, 3.5.12).

Le temps de tolérance d'erreurs du système général doit alors être supérieur à la somme des temps de réaction ou des intervalles d'essai de diagnostic de tous les composants de la chaîne de mesure de sécurité. La caractéristique correspondante est la valeur PFH.

3.3 Types d'erreur

Une défaillance non dangereuse (safe failure) n'entraîne pas le basculement du système de sécurité dans un état dangereux ou dans un état de dysfonctionnement. Le convertisseur bascule dans l'état sûr défini ou dans le mode de perturbation en cas de dépassement de la plage de mesure, par ex. 21 mA.

Une défaillance dangereuse non détectée (dangerous undetected failure) peut entraîner le basculement du système de sécurité dans un état dangereux ou dans un état de dysfonctionnement. Le convertisseur ne bascule pas dans l'état sûr défini ou dans le mode de perturbation.

3.4 Intervalle d'essai de diagnostic

Parallèlement aux fonctions de sécurité à proprement parler, des fonctions de diagnostic sont continuellement exécutées dans les convertisseurs afin de détecter tout comportement défaillant. L'intervalle d'essai de diagnostic représente la période pendant laquelle ces essais sont réalisés et répétés. Des erreurs de matériel fortuites sont détectées pendant cette période.

4 Montage et installation

Selon le modèle de convertisseur, les documentations suivantes doivent être jointes :

PolyTrans® P32000P0/1x	ThermoTrans® P32100P0/1x	SensoTrans® P32200P0/1x	SensoTrans® P32300P0/1x
Mode d'emploi TA-254.111-KNxxx	Mode d'emploi TA-254.113-KNxxx	Mode d'emploi TA-254.114-KNxxx	Mode d'emploi TA-254.115-KNxxx

Les consignes, les conditions générales et les valeurs limites indiquées dans les modes d'emploi doivent être respectées lors de l'installation et de l'utilisation des convertisseurs.

Les appareils pour lesquels un très haut degré de disponibilité est nécessaire doivent être affectés à la catégorie de surtension III. Avec la catégorie de surtension III et le degré de pollution 2, la tension de service maximale admissible est de 150 VCA/CC. Si la tension de service est > 150 VCA/CC, il est nécessaire de prendre des mesures adaptées de protection contre la surtension afin de s'assurer que la catégorie de surtension III est respectée.

Les câbles reliant le capteur situé sur le point de mesure au convertisseur doivent être disposés de manière à empêcher un court-circuit entre les fils et avec l'environnement des câbles.

Pour un type de signal de sortie configuré Courant (par ex. 4 … 20 mA), la charge de sortie doit être ≥ 50 Ω.

Avant la mise en service et après chaque modification de la programmation, vérifier le fonctionnement conforme du convertisseur (cf. chapitre 5.1 "Vérification du fonctionnement").

Si la programmation a été effectuée par le biais de l'interface IrDA®, le convertisseur doit ensuite être placé en mode Read-Only. Dans ce mode de fonctionnement, les données peuvent uniquement être envoyées par le convertisseur via l'interface IrDA® (affichage des mesures, statistiques, ...).

Activer le mode Read-Only :

- Tous les commutateurs DIP = 0
- Tous les commutateurs rotatifs = 0

Une fois la programmation correctement effectuée, fixer les commutateurs à l'aide du film en polyimide autocollant fourni.

5 Contrôles périodiques

Le contrôle de fonctionnement périodique permet de détecter d'éventuelles erreurs dangereuses non détectables par l'auto-diagnostic. Le bon fonctionnement du convertisseur doit donc être vérifié à des intervalles réguliers et appropriés.

C'est à l'utilisateur que revient la responsabilité de choisir le mode de contrôle et les intervalles. Les intervalles de contrôle sont entre autres déterminés lors du calcul de chaque circuit de sécurité d'une installation (valeurs PFD).

Le contrôle doit être réalisé de manière à démontrer le bon fonctionnement de la fonction de sécurité en interaction avec tous les composants.

5.1 Vérification du fonctionnement

Les valeurs PFD documentées dans le chapitre 6.x s'appliquent à l'intervalle de contrôle TI = 1 an. Le bon fonctionnement du convertisseur doit être vérifié dans l'application. Pour cela, procéder comme suit :

- Activer le convertisseur avec la sortie ouverte (charge = ∞).
  Vérifier les messages d'état et de diagnostic signalés par des LED :
  - Aucune erreur d'appareil ne doit être signalée (message d'erreur 10).
  - Pour le type de signal de sortie configuré Courant (par ex. 4 … 20 mA), le message d'erreur 6 (erreur de sortie Charge) doit être signalé.
- Spécifier des valeurs de consigne pour le début et la fin de la plage de mesure, ainsi qu'une valeur moyenne (par ex. valeur 50 %). Vérifier que l'écart de mesure est compris dans les tolérances spécifiées.
- Vérifier que le basculement dans l'état sûr s'effectue correctement. Pour le vérifier, privilégier la simulation d'une rupture de câble (entrée ouverte). La sortie commande alors à ≥ 21 mA (sorties de courant) ou ≥ 5,25 V ou ≥10,5 V (sorties de tension). Le message d'erreur "Capteur ouvert" est alors transmis (la LED rouge clignote 4 fois).

Le signal d'erreur est maintenu même si la cause de l'erreur a été résolue (message d'erreur auto-maintenu). Le message d'erreur est réinitialisé par un redémarrage (marche/arrêt de l'énergie auxiliaire ou via l'IrDA).

Si l'essai de fonctionnement s'avère négatif, le convertisseur doit être mis hors service et le processus doit être maintenu dans un état sûr par le biais d'autres mesures.

Le convertisseur lui-même ne nécessite pas d'entretien.

6 Caractéristiques de sécurité

6.1 Suppositions

- La communication par le biais de l'interface IrDA est exclusivement utilisée pour la configuration de l'appareil ou pour des fonctions de diagnostic, mais pas pour des opérations critiques de sécurité.
- Après la configuration (avec des commutateurs rotatifs/DIP ou l'interface IrDA), un contrôle de fonctionnement est réalisé afin de vérifier que la fonction de mesure exécutée est conforme aux spécifications.
- Le temps de résolution (MTTR) après une erreur d'appareil ne dépasse pas 72 heures.
- La température moyenne considérée sur une longue période ne dépasse pas 55°C.
- Les conditions ambiantes correspondent aux conditions moyennes d'un environnement industriel.
- Les spécifications du mode d'emploi ne doivent pas être dépassées.

6.2 Caractéristiques spécifiques de sécurité

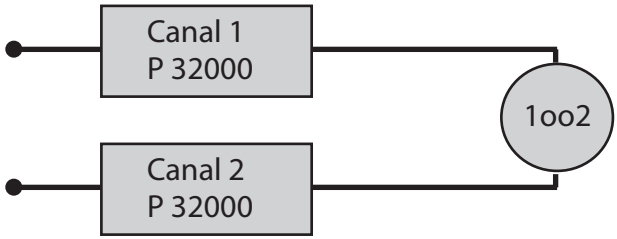
Structure	1 canal (1oo1)
Catégorie	SIL 2 (logiciel SIL 3)
Type d'appareil	Type B
HFT	0
SFF	97 %
DC	94 %
β	2 %
β_D	1 %
MTTR	72 h
PFD_{SIL2}	$2{,}7 \cdot 10^{-4}$
PFH_{SIL2}	$4{,}8 \cdot 10^{-8}$/h
PFD_{SIL3}	$4{,}9 \cdot 10^{-6}$
PFH_{SIL3}	$8{,}5 \cdot 10^{-9}$/h
Intervalle d'essai de diagnostic	< 5 s
Temps de réaction aux erreurs en cas de dépassement positif ou négatif de la plage de mesure	< 2 s
Taux de défaillance :	
λ_S	759,2 FIT
λ_D	759,2 FIT
λ_{DU}	48,1 FIT
λ_{DD}	711,1 FIT

Remarque :
Le taux de défaillance des éléments électroniques augmente après une durée d'utilisation de 8 à 12 ans, ce qui entraîne une altération des valeurs PFD et PFH qui en sont dérivées (DIN EN 61508-2, 7.4.7.4, remarque 3).

6.3 Exemple de calcul

Un système doublement redondant avec deux convertisseurs PolyTrans P32000® est supposé à titre d'exemple de calcul concret (système 1oo2). L'intervalle de contrôle T_I est de 1 an (8760 h).

Afin que la fonction de sécurité soit correctement exécutée, les canaux doit être reliés entre eux de manière à ce que l'un des canaux suffise au déclenchement de la fonction de sécurité. Dans un système 1oo2, cela provoque donc une défaillance dangereuse de la fonction de sécurité si les deux canaux sont simultanément défaillants.



Equation de détermination de PFD pour un système 1oo2 :

$$PFD_{G,1002} = 2\,((1-\beta)\,\lambda_{DD} + (1-\beta)\,\lambda_{DU})^2\,t_{CE}\,t_{GE} + \beta_D\lambda_D MTTR + \beta\lambda_{DU}\left(\frac{T_I}{2} + MTTR\right)$$

avec

$$T_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left[\frac{T_I}{2} + MTTR\right] + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR$$

$$T_{GE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left[\frac{T_I}{3} + MTTR\right] + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR$$

Equation de détermination de PFH pour un système 1oo2 :

$$PFG_{G,1002} = 2\,((1-\beta_D)\,\lambda_{DD} + (1-\beta)\,\lambda_{DU})^2\,t_{CE} + \beta_D\lambda_{DD} + \beta\lambda_{DU}$$

avec

$$T_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left[\frac{T_I}{2} + MTTR\right] + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR$$

Les valeurs suivantes sont obtenues pour ce système :

Structure	2 canaux (1oo2)
Catégorie	SIL 3
Architecture	Type B
HFT	1
SFF	97 %
DC	94 %
β	2 %
β_D	1 %
MTTR	72 h
t_{CE}	349,5 h
t_{GE}	67,5 h
$PFD_{G,1oo2}$	$4{,}9 \cdot 10^{-6}$
$PFH_{G,1oo2}$	$8{,}5 \cdot 10^{-9}$/h

TÜVRheinland®
Genau. Richtig.

ZERTIFIKAT
CERTIFICATE

Nr./No. 968/EZ 272.00/07

Prüfgegenstand **Product tested**	Messumformer-Reihe P32000	**Zertifikatsinhaber** **Holder of the certificate**	Knick Elektronische Messgeräte GmbH & Co. KG Beuckestrasse 22 14163 Berlin
Typbezeichnung **Type designation**	PolyTrans® P 32000 P0/1* SensoTrans® R P 32300 P0/1* SensoTrans® DMS P 32200 P0/1* ThermoTrans® P 32100 P0/1*	**Verwendungs-zweck** **Intended application**	Einsatz als Teil von Schutzein-richtungen zur Überwachung sicherheitsrelevanter Signale (Temperatur, Widerstand, Potentiometer, Spannung, ...)
Prüfgrundlagen **Codes and standards forming the basis of testing**	EN 61508:2001 EN 61511:2004 EN 61010-1:2001 EN 61326-1:2006 IEC 61326-3-2:2006 EN 50178:1997		
Prüfungsergebnis **Test results**	Die Messumformer-Reihe P32000 mit den oben genannten Typen erfüllt die gestellten Anforderungen der EN 61508 für SIL 2 bzw. SIL 3 im redundanten Betrieb und können in Schutzeinrichtungen zur Überwachung von sicherheitsrelevanten Prozessgrössen ein-gesetzt werden.		
Besondere Bedingungen **Specific requirements**	Die Sicherheitshinweise im Sicherheitshandbuch und in den Gebrauchsanleitungen der Messumformer sind zu berück-sichtigen.		

Functional Safety
Type Approved
TÜVRheinland® FS

Der Prüfbericht-Nr.: 968/EZ 272.00/07 vom 12.10.2007 ist Bestandteil dieses Zertifikates.
Der Inhaber eines für den Prüfgegenstand gültigen Genehmigungs-Ausweises ist berechtigt, die mit dem Prüfgegenstand übereinstimmenden Erzeugnisse mit dem abgebildeten Prüfzeichen zu versehen.

The test report-no.: 968/EZ 272.00/07 dated 12.10.2007 is an integral part of this certificate.
The holder of a valid licence certificate for the product tested is authorized to affix the test mark shown opposite to products, which are identical with the product tested.

TÜV Rheinland Industrie Service GmbH
Geschäftsfeld ASI
Automation, Software und Informationstechnologie
Am Grauen Stein, 51105 Köln
Postfach 91 09 51, 51101 Köln

12.10.2007
Datum/Date

Firmenstempel/Company Seal

Dipl.-Ing. Klaus Kemp

Knick
Elektronische Messgeräte GmbH & Co. KG
P.O. Box 37 04 15
D-14134 Berlin
Tél. : +49 (0)30 - 801 91 - 0
Fax : +49 (0)30 - 801 91 - 200
Internet : http://www.knick.de
knick@knick.de

TS-254.111-KNF01 20071009